

Attachment C



Washington, D.C. 20530

December 24, 2002

MEMORANDUM FOR

MICHAEL CHERTOFF
ASSISTANT ATTORNEY GENERAL
CRIMINAL DIVISION


JAMES BAKER
COUNSEL FOR INTELLIGENCE POLICY
OFFICE OF INTELLIGENCE POLICY AND REVIEW

ALL UNITED STATES ATTORNEYS

ALL ANTI-TERRORISM TASK FORCE COORDINATORS

ALL SPECIAL AGENTS
FEDERAL BUREAU OF INVESTIGATION

FROM:

THE DEPUTY ATTORNEY GENERAL 
DIRECTOR, FEDERAL BUREAU OF INVESTIGATION

SUBJECT:

Field Guidance on Intelligence Sharing Procedures for
FI and FCI Investigations

The Foreign Intelligence Surveillance Court of Review issued an opinion on November 18, 2002, that authorizes unprecedented coordination between criminal investigators and prosecutors and intelligence agents in the conduct of foreign intelligence (FI) and foreign counterintelligence (FCI) investigations. This opinion removes the "wall" that previously limited such coordination in investigations in which agents employed, or contemplated employing, electronic surveillance or physical search authority pursuant to the Foreign Intelligence Surveillance Act (FISA). The Court of Review approved Intelligence Sharing Procedures permitting such coordination that were issued by the Attorney General on March 6, 2002 (attached). The accompanying memorandum, entitled A Summary of the FISA Appeal Decision, discusses the legal reasoning and implications of the Court of Review's decision. This memorandum summarizes the Attorney General's March 2002 Intelligence Sharing Procedures that now govern FI and FCI investigations conducted by the FBI.¹

¹ Because the Court of Review approved the Attorney General's March 2002 Procedures, the interim guidance that was issued while the appeal was pending – including the July 17, 2002

Subject: Field Guidance on Intelligence Sharing Procedures for FI and FCI Investigations

Under the March 2002 Procedures, FBI intelligence agents must disseminate to criminal prosecutors all relevant foreign intelligence information, including information obtained from FISA, in accordance with applicable minimization standards and other specific restrictions (e.g., originator controls). Correspondingly, prosecutors and criminal agents may advise FBI intelligence agents on all aspects of FI and FCI investigations, including the use of FISA. In other words, a criminal prosecutor or agent may nominate or suggest a particular individual as a FISA target, even if that prosecutor or agent hopes to secure a criminal indictment against that target.

The March 2002 Procedures cite four limitations on the sharing of this information: (1) All information that is shared with a United States Attorney's Office (USAO) pursuant to the Procedures shall be disseminated only to the United States Attorney or to a designated AUSA with appropriate clearances and training in the handling of such information. (2) In espionage investigations, absent an emergency, the FBI must first contact the Criminal Division before sharing information and/or consulting with a USAO. (3) Absent an emergency, prosecutors may not use any information obtained from an FI or FCI investigation in any proceeding (including a grand jury proceeding or a warrant application) or disclose it to any court without first consulting with OIPR and the Criminal Division. (4) Where such information is obtained or derived from FISA, it may not be used in any proceeding (including a grand jury proceeding or a warrant application) without the advance authorization of the Attorney General, which shall be obtained through the FBI's National Security Law Unit (NSLU) and OIPR, with simultaneous notice to the Criminal Division.

Although consultations and information-sharing with prosecutors may now take place without prior notice to OIPR (or reporting to the Foreign Intelligence Surveillance Court), the March 2002 Intelligence Sharing Procedures provide that "[c]onsistent with * * * standards of effective management, all relevant DOJ components," including OIPR, "must be fully informed about the nature, scope, and conduct" of FI and FCI investigations, so that all components are in a position to "offer advice * * * about the conduct and goals of the investigations." For the same reasons, NSLU must be kept fully informed. In pursuing our mission, we must use all available resources, intelligence and law enforcement alike, to protect the country and recognize that prosecution is one way, but only one way, to combat espionage and terrorism.

Accordingly, a law enforcement agent or prosecutor may not discourage or prevent the FBI from disseminating to the U.S. Intelligence Community (IC) or to OIPR all relevant foreign intelligence information obtained from an FI or FCI investigation, even if it is believed that such dissemination might jeopardize a possible prosecution, except in those rare cases where the Attorney General has formally authorized such a restriction. Agents or prosecutors who believe that such a restriction is appropriate should contact the Criminal Division.

memorandum from Assistant Attorney General Michael Chertoff entitled Review of FBI Intelligence Files, and the September 18, 2002 EC to all FBI Field Offices from the Office of the General Counsel – is now superseded by the March 2002 Procedures.

Subject: Field Guidance on Intelligence Sharing Procedures for FI and FCI Investigations

In deciding whether to request initiation or renewal of FISA authority, all Department personnel must bear in mind two important requirements. First, there must be at least a "significant" non-prosecutorial purpose for every FISA application. Second, FISA may be used primarily to obtain evidence for use in a prosecution, but only if the prosecution concerns an offense related to the foreign intelligence threat posed by the FISA target – i.e., espionage, terrorism, or other offenses related to the foreign intelligence threat, such as bank robbery committed to finance or facilitate espionage or terrorism. These limits are discussed in detail in the accompanying memorandum, A Summary of the FISA Appeal Decision. As a practical matter, they should not hinder coordination between intelligence and law enforcement officials.²

² This memorandum, and the March 2002 Intelligence Sharing Procedures, have been promulgated solely for the purpose of internal Department of Justice guidance. They are not intended to, do not, and may not be relied upon to create any rights, substantive or procedural, that are enforceable at law by any party in any matter, civil or criminal, nor do they place any limitations on otherwise lawful investigative or litigative prerogatives of the Department.

Subject: Field Guidance on Intelligence Sharing Procedures for FI and FCI Investigations

This chart presents the basic rules in the March 2002 Intelligence Sharing Procedures. Consult the Procedures themselves, or contact OIPR or NSLU, for more detailed guidance.

	SHARING INFORMATION	USING INFORMATION	GIVING ADVICE
TERRORISM CASES	The FBI must keep a designated AUSA in the relevant USAO, OIPR, and CRM fully informed of all relevant foreign intelligence information, as well as evidence of any crime, including information and evidence obtained or derived from FISA. Information obtained or derived from FISA shall be marked as required in 50 U.S.C. §§ 1806(b) and 1825(c).	Prosecutors may disclose or use such information in any proceeding after coordination with CRM and OIPR. Prosecutors may use information obtained or derived from FISA in any proceeding with prior AG approval.	Prosecutors may give any advice, including advice on the use of FISA, but may not discourage sharing information with the IC absent AG approval. Agents and prosecutors may consult without advance notice to OIPR. However, all relevant DOJ components must be fully informed about investigations so that they can offer advice on the conduct and goals of those investigations.
ESPIONAGE CASES	The FBI must keep OIPR and CRM fully informed of all relevant foreign intelligence information, as well as evidence of any crime, including information and evidence obtained or derived from FISA. Absent emergency, the FBI shall consult with CRM before providing information or evidence to a designated AUSA in the relevant USAO. Information obtained or derived from FISA shall be marked as required in 50 U.S.C. §§ 1806(b) and 1825(c).	Prosecutors may disclose or use such information in any proceeding after coordination with CRM and OIPR. Prosecutors may use information obtained or derived from FISA in any proceeding with prior AG approval.	CRM, and with CRM's approval, a designated AUSA in the relevant USAO, may give any advice, including advice on the use of FISA, but may not discourage sharing information with the IC absent AG approval. Agents and prosecutors may consult without advance notice to OIPR. However, all relevant DOJ components must be fully informed about investigations so that they can offer advice on the conduct and goals of those investigations.



Office of the Attorney General
Washington, D. C. 20530

March 6, 2002

MEMORANDUM

TO: Director, FBI
Assistant Attorney General, Criminal Division
Counsel for Intelligence Policy
United States Attorneys

FROM: The Attorney General *John Ashcroft*

SUBJECT: Intelligence Sharing Procedures for Foreign
Intelligence and Foreign Counterintelligence
Investigations Conducted by the FBI

I. INTRODUCTION AND STATEMENT OF GENERAL PRINCIPLES

Unless otherwise specified by the Attorney General, these procedures apply to foreign intelligence (FI) and foreign counterintelligence (FCI) investigations conducted by the Federal Bureau of Investigation (FBI). They are designed to ensure that FI and FCI investigations are conducted lawfully, particularly in light of requirements imposed by the Foreign Intelligence Surveillance Act (FISA), and to promote the effective coordination and performance of the criminal and counterintelligence functions of the Department of Justice (DOJ). These procedures supersede the procedures adopted by the Attorney General on July 19, 1995 (including the annex concerning the Southern District of New York), the interim measures approved by the Attorney General on January 21, 2000, and the memorandum issued by the Deputy Attorney General on August 6, 2001. Terms used in these procedures shall be interpreted in keeping with definitions contained in FISA. References in these procedures to particular positions or components within the Department of Justice shall apply to any successor position or component.

Prior to the USA Patriot Act, FISA could be used only for the "primary purpose" of obtaining "foreign intelligence information." The term "foreign intelligence information" was and is defined to include information that is necessary, or relevant, to the ability of the United States to protect against

foreign threats to national security, such as attack, sabotage, terrorism, or clandestine intelligence activities. See 50 U.S.C. § 1801(e)(1). Under the primary purpose standard, the government could have a significant law enforcement purpose for using FISA, but only if it was subordinate to a primary foreign intelligence purpose. The USA Patriot Act allows FISA to be used for "a significant purpose," rather than the primary purpose, of obtaining foreign intelligence information. Thus, it allows FISA to be used primarily for a law enforcement purpose, as long as a significant foreign intelligence purpose remains. See 50 U.S.C. §§ 1804(a)(7)(B), 1823(a)(7)(B).

The Act also expressly authorizes intelligence officers who are using FISA to "consult" with federal law enforcement officers to "coordinate efforts to investigate or protect against" foreign threats to national security. Under this authority, intelligence and law enforcement officers may exchange a full range of information and advice concerning such efforts in FI or FCI investigations, including information and advice designed to preserve or enhance the possibility of a criminal prosecution. The USA Patriot Act provides that such consultation between intelligence and law enforcement officers "shall not" preclude the government's certification of a significant foreign intelligence purpose or the issuance of a FISA warrant. See 50 U.S.C. §§ 1806(k), 1825(k).

Consistent with the USA Patriot Act and with standards of effective management, all relevant DOJ components, including the Criminal Division, the relevant United States Attorney's Offices (USAOs), and the Office of Intelligence Policy and Review (OIPR), must be fully informed about the nature, scope, and conduct of all full field FI and FCI investigations, whether or not those investigations involve the use of FISA. Correspondingly, the Attorney General can most effectively direct and control such FI and FCI investigations only if all relevant DOJ components are free to offer advice and make recommendations, both strategic and tactical, about the conduct and goals of the investigations. The overriding need to protect the national security from foreign threats compels a full and free exchange of information and ideas.

II. INTELLIGENCE SHARING PROCEDURES CONCERNING THE CRIMINAL DIVISION

A. Disseminating Information.

The Criminal Division and OIPR shall have access to all information developed in full field FI and FCI investigations

except as limited by orders issued by the Foreign Intelligence Surveillance Court, controls imposed by the originators of sensitive material, and restrictions established by the Attorney General or the Deputy Attorney General in particular cases. See 50 U.S.C. §§ 1801(h), 1806(a), 1825(a).

The FBI shall keep the Criminal Division and OIPR apprised of all information developed in full field FI and FCI investigations that is necessary to the ability of the United States to investigate or protect against foreign attack, sabotage, terrorism, and clandestine intelligence activities, subject to the limits set forth above. Relevant information includes both foreign intelligence information and information concerning a crime which has been, is being, or is about to be committed. The Criminal Division and OIPR must have access to this information to ensure the ability of the United States to coordinate efforts to investigate and protect against foreign threats to national security, including protection against such threats through criminal investigation and prosecution, and in keeping with the need of the United States to obtain, produce, and disseminate foreign intelligence information. See 50 U.S.C. §§ 1801(h)(1), 1806(k), 1825(k).

The FBI shall also keep the Criminal Division and OIPR apprised of information developed in full field FI and FCI investigations that concerns any crime which has been, is being, or is about to be committed. See 50 U.S.C. § 1801(h)(3).

As part of its responsibility under the preceding paragraphs, the FBI shall provide to the Criminal Division and OIPR copies of annual Letterhead Memoranda (or successor summary documents) in all full field FI and FCI investigations, and shall make available to the Criminal Division and OIPR relevant information from investigative files, as appropriate. The Criminal Division shall adhere to any reasonable conditions on the storage and disclosure of such documents and information that the FBI or OIPR may require.

All information acquired pursuant to a FISA electronic surveillance or physical search that is disseminated to the Criminal Division shall be accompanied by a statement that such information, or any information derived therefrom, may only be used in any criminal proceeding (including search and arrest warrant affidavits and grand jury subpoenas and proceedings) with the advance authorization of the Attorney General. See 50 U.S.C. §§ 1806(b), 1825(c).

B. Providing Advice.

The FBI, the Criminal Division, and OIPR shall consult with one another concerning full field FI and FCI investigations except as limited by these procedures, orders issued by the Foreign Intelligence Surveillance Court, and restrictions established by the Attorney General or the Deputy Attorney General in particular cases.

Consultations may include the exchange of advice and recommendations on all issues necessary to the ability of the United States to investigate or protect against foreign attack, sabotage, terrorism, and clandestine intelligence activities, including protection against the foregoing through criminal investigation and prosecution, subject to the limits set forth above. Relevant issues include, but are not limited to, the strategy and goals for the investigation; the law enforcement and intelligence methods to be used in conducting the investigation; the interaction between intelligence and law enforcement components as part of the investigation; and the initiation, operation, continuation, or expansion of FISA searches or surveillance. Such consultations are necessary to the ability of the United States to coordinate efforts to investigate and protect against foreign threats to national security as set forth in 50 U.S.C. §§ 1806(k), 1825(k).

The FBI, the Criminal Division, and OIPR shall meet regularly to conduct consultations. Consultations may also be conducted directly between two or more components at any time. Disagreements arising from consultations may be presented to the Deputy Attorney General or the Attorney General for resolution.

III. INTELLIGENCE SHARING PROCEDURES CONCERNING A USAO

With respect to FI or FCI investigations involving international terrorism, the relevant USAOs shall receive information and engage in consultations to the same extent as the Criminal Division under Parts II.A and II.B of these procedures. Thus, the relevant USAOs shall have access to information developed in full field investigations, shall be kept apprised of information necessary to protect national security, shall be kept apprised of information concerning crimes, shall receive copies of LHMs or successor summary documents, and shall have access to FBI files to the same extent as the Criminal Division. The relevant USAOs shall receive such information and access from the FBI field offices. The relevant USAOs also may and shall engage in regular consultations with the FBI and OIPR to the same extent as the Criminal Division.

With respect to FI or FCI investigations involving espionage, the Criminal Division shall, as appropriate, authorize the dissemination of information to a USAO, and shall also, as appropriate, authorize consultations between the FBI and a USAO, subject to the limits set forth in Parts II.A and II.B of these procedures. In an emergency, the FBI may disseminate information to, and consult with, a United States Attorney's Office concerning an espionage investigation without the approval of the Criminal Division, but shall notify the Criminal Division as soon as possible after the fact.

All information disseminated to a USAO pursuant to these procedures, whether or not the information is derived from FISA and whether or not it concerns a terrorism or espionage investigation, shall be disseminated only to the United States Attorney (USA) and/or any Assistant United States Attorneys (AUSAs) designated to the Department of Justice by the USA as points of contact to receive such information. The USAs and the designated AUSAs shall have appropriate security clearances and shall receive training in the handling of classified information and information derived from FISA, including training concerning restrictions on the use and dissemination of such information.

Except in an emergency, where circumstances preclude the opportunity for consultation, the USAOs shall take no action on the information disseminated pursuant to these procedures without consulting with the Criminal Division and OIPR. The term "action" is defined to include the use of such information in any criminal proceeding (including search and arrest warrant affidavits and grand jury subpoenas and proceedings), and the disclosure of such information to a court or to any non-government personnel. See also U.S. Attorney's Manual §§ 9-2.136, 9-90.020. Disagreements arising from consultations pursuant to this paragraph may be presented to the Deputy Attorney General or the Attorney General for resolution.

All information acquired pursuant to a FISA electronic surveillance or physical search that is disseminated to a USAO shall be accompanied by a statement that such information, or any information derived therefrom, may only be used in any criminal proceeding (including search and arrest warrant affidavits and grand jury subpoenas and proceedings) with the advance authorization of the Attorney General. See 50 U.S.C. §§ 1806(b), 1825(c). Whenever a USAO requests authority from the Attorney General to use such information in a criminal proceeding, it shall simultaneously notify the Criminal Division.



U.S. Department of Justice

Office of the Deputy Attorney General

The Deputy Attorney General

Washington, D.C. 20530

December 24, 2002

MEMORANDUM FOR

MICHAEL CHERTOFF
ASSISTANT ATTORNEY GENERAL
CRIMINAL DIVISION

JAMES BAKER
COUNSEL FOR INTELLIGENCE POLICY
OFFICE OF INTELLIGENCE POLICY AND REVIEW

ALL UNITED STATES ATTORNEYS

ALL ANTI-TERRORISM TASK FORCE COORDINATORS

ALL SPECIAL AGENTS
FEDERAL BUREAU OF INVESTIGATION

FROM:

LARRY D. THOMPSON

SUBJECT:

A Summary of the FISA Appeal Decision

This memorandum summarizes and explains the reasoning of the Foreign Intelligence Surveillance Court of Review's decision of November 18, 2002, which approved Intelligence Sharing Procedures promulgated by the Attorney General on March 6, 2002. The accompanying memorandum, entitled Field Guidance on Intelligence Sharing Procedures for FI and FCI Investigations, summarizes the Attorney General's March 2002 Intelligence Sharing Procedures that now govern foreign intelligence (FI) and foreign counterintelligence (FCI) investigations conducted by the FBI.

1. The Foreign Intelligence Surveillance Act (FISA), 50 U.S.C. §§ 1801-1829, governs electronic surveillance and physical searches of foreign powers and their agents inside the United States. Although "in many respects" FISA sets standards that are "equivalent" to those governing electronic surveillance and physical searches in ordinary criminal cases, there are important differences.

Subject: A Summary of the FISA Appeal Decision

Court of Review Opinion at 48. In some respects, FISA lacks protections that apply in ordinary criminal cases, while in other respects it “contains additional protections.” *Id.* at 49.¹

The recent appeal to the Foreign Intelligence Surveillance Court of Review concerned one of those additional protections in FISA – a requirement concerning the “purpose” of a search or surveillance conducted under the statute. As enacted in 1978, FISA provided that “the purpose” of a surveillance must be to obtain “foreign intelligence information.” 50 U.S.C. § 1804(a)(7)(B). The term “foreign intelligence information” was (and is) defined to include information necessary to “protect” against certain specified foreign threats to national security, including attack, sabotage, international terrorism, and espionage committed by foreign powers or agents of foreign powers. 50 U.S.C. § 1801(e)(1). The definition does not limit the ways in which foreign intelligence information may be used to protect national security – i.e., it does not discriminate among otherwise lawful methods of neutralizing the specified threats.

Historically, courts interpreted these provisions in particular ways. First, they read FISA’s “the purpose” language to require that “the primary purpose” of a search or surveillance be to obtain foreign intelligence information. Second, they treated “foreign intelligence information” as if it did not include information necessary to protect against the specified foreign threats to national security using law enforcement methods (e.g., prosecuting a foreign spy or terrorist) as opposed to non-law enforcement, traditional intelligence methods (e.g., recruiting a foreign spy or terrorist as a double agent). Under this regime, FISA could be used for a significant, albeit secondary, purpose to obtain evidence for use in a prosecution, as long the government’s primary purpose was to gather information for use in non-law enforcement methods.

Courts determined the government’s “primary purpose” for using FISA by examining the degree of coordination between intelligence and law enforcement officials. The more coordination that occurred – the more information and advice exchanged between intelligence and law enforcement officials – the more likely courts were to find that the government’s primary purpose in seeking a FISA was law enforcement, and to deny the application for that reason. As the Court of Review explained in its opinion, the Foreign Intelligence Surveillance Court (FISC) “determined an investigation became primarily criminal when the Criminal Division [or a U.S. Attorney’s office] played a lead role.” Opinion at 52. This created “perverse organizational incentives,” expressly discouraging coordination in the fight against terrorism. *Ibid.*

¹ One additional protection in FISA is the requirement that the statute may only be used to target a “foreign power” or an “agent of a foreign power” as defined in 50 U.S.C. § 1801(a)-(b). That requirement, which was not changed by the USA Patriot Act or by the government’s appeal, means that the government cannot use FISA to target ordinary U.S. persons not connected to a foreign power, even if they are committing serious crimes such as murder or domestic terrorism.

Subject: A Summary of the FISA Appeal Decision

2. The USA Patriot Act directly addressed FISA's purpose requirement and the problem of coordination. First, it changed "the purpose" to "a significant purpose." Second, it expressly authorized intelligence officers who are using FISA to "consult" with federal law enforcement officers to "coordinate" their respective efforts to "protect" national security against the list of threats contained in the definition of "foreign intelligence information" – i.e., attack, sabotage, international terrorism, and espionage committed by foreign powers or agents of foreign powers. 50 U.S.C. §§ 1806(k), 1825(k). The Patriot Act provided that such coordination "shall not" preclude the government's certification or the FISC's finding of the required "significant" purpose to obtain foreign intelligence information. *Ibid.*

To implement these provisions of the USA Patriot Act, the Attorney General adopted new Intelligence Sharing Procedures on March 6, 2002. The March 2002 Procedures provide that "all relevant DOJ components," intelligence and law enforcement, "must be fully informed" concerning FI and FCI investigations, and that all components must also be "free to offer advice and make recommendations, both strategic and tactical, about the conduct and goals of the investigations." In an opinion issued on May 17, 2002, the FISC accepted in part and rejected in part the Attorney General's March 2002 Procedures, limiting the advice that prosecutors may provide to intelligence officials, and imposing a "chaperone" requirement under which the Office of Intelligence Policy and Review (OIPR) was required to receive notice of, and participate in, all consultations between intelligence agents and prosecutors unless it was "unable" to do so. The government then appealed to the Court of Review.

3. The Court of Review rejected the FISC's analysis, including the "chaperone" requirement, and approved the Department's March 2002 Procedures in full. It held that FISA allows complete coordination between intelligence and law enforcement officials, even if such coordination results in what might be characterized as law enforcement "direction" or "control" of an investigation. Opinion at 23, 32. Under the Court of Review's decision, FISA may be used primarily for the purpose of obtaining evidence to prosecute a foreign spy or terrorist, and prosecutors may provide any advice, including advice on the use of FISA itself, in furtherance of such a purpose. *Ibid.* The Court found "simply no basis" for the FISC's decision "to limit criminal prosecutors' ability to advise FBI intelligence officials on the initiation, operation, continuation, or expansion of FISA surveillances to obtain foreign intelligence information, even if such information includes evidence of a foreign intelligence crime." *Id.* at 27-28. Indeed, the Court of Review stated that in doing so the FISC "may well have exceeded the constitutional bounds that restrict an Article III court." *Id.* at 28. The Court's decision changes both the purpose for which the government may use FISA, and the nature and scope of judicial review of that purpose.

a. The Court of Review concluded that "the obvious reading" of FISA as enacted in 1978 is that "foreign intelligence information" includes information sought for use as evidence in a prosecution for espionage or terrorism. Opinion at 12. The Court explained: "The government argues persuasively that arresting and prosecuting terrorist agents of, or spies for, a foreign power may be the best

Subject: A Summary of the FISA Appeal Decision

technique to prevent them from successfully continuing their terrorist or espionage activity.” *Id.* at 13. In other words, prosecuting a spy or terrorist is one way to “protect” national security under 50 U.S.C. § 1801(e)(1). Indeed, based on FISA’s legislative history, the Court found that “Congress actually anticipated the government’s argument and explicitly approved it.” *Ibid.* The Court thus rejected the “false dichotomy between foreign intelligence information that is evidence of foreign intelligence crimes and that which is not.” *Id.* at 15. Prosecution of a spy or terrorist is itself a legitimate “foreign intelligence purpose” under FISA as enacted in 1978.

The Court identified two limits on the use of FISA. First, because of the USA Patriot Act, there must be at least a “significant” non-law enforcement purpose for every FISA application. In other words, a significant purpose of every FISA must be to obtain “foreign intelligence information” for use in protecting national security through methods other than criminal prosecution – *e.g.*, recruiting a foreign spy as a double agent. More generally, of course, detection of espionage or terrorist communications networks, taskings, and other tradecraft will invariably assist in developing appropriate diplomatic, military, economic, or other non-law enforcement countermeasures. Use of these or other non-law enforcement countermeasures must be at least a significant purpose for conducting a search or surveillance under FISA.²

Second, the Court held that FISA may be used primarily to obtain evidence for a criminal prosecution (Opinion at 34), but only if the prosecution concerns an offense related to a foreign intelligence threat. The Court divided crimes into two categories: “foreign intelligence crimes” and “ordinary crimes.” A foreign intelligence crime is any crime “referred to in section 1801(a)-(e)” of FISA – *i.e.*, espionage and international terrorism, unlawful clandestine intelligence activities, sabotage, identity fraud offenses committed for or on behalf of a foreign power, and aiding and abetting or conspiring to commit these offenses. Opinion at 11. Moreover, any crime inextricably intertwined with foreign intelligence activity – such as a bank robbery committed to finance terrorist activity, or credit card fraud designed to maintain the cover of a sleeper spy – is also a foreign intelligence crime. *Id.* at 37. By contrast, an ordinary crime is one “‘totally unrelated to intelligence matters,’” *id.* at 27 (quoting FISA’s 1978 legislative history), such as when a foreign spy murders his wife to be with his mistress, or when an international terrorist is also a consumer of child pornography. FISA may be used primarily to

² The Court arrived at this conclusion by attributing to Congress in passing the USA Patriot Act an intent to perpetuate the dichotomy between foreign intelligence and law enforcement. Although Congress did not adopt the dichotomy when it enacted FISA in 1978, the Patriot Act implicitly codified the dichotomy because it was enacted against the background of (incorrect) judicial and executive interpretations adopting the dichotomy. Thus, the Court explained, “even though we agree that the original FISA did not contemplate the ‘false dichotomy,’ the Patriot Act actually did – which makes it no longer false.” Opinion at 35.

Subject: A Summary of the FISA Appeal Decision

obtain evidence of a foreign intelligence crime, but not of an ordinary crime. Of course, evidence of any crime obtained or derived from a lawful FISA search or surveillance may be used in a subsequent prosecution; the limit applies only to the government's purpose and intent to use information at the time it seeks and conducts the search or surveillance.

These two requirements should not inhibit necessary coordination between intelligence and law enforcement officials. As to the first requirement, even when the government's prosecutorial purpose is at its zenith, there will still always (or almost always) be a significant non-prosecutorial purpose for conducting a FISA search or surveillance. Indeed, the Court of Review itself recognized that this requirement "may not make much practical difference." Opinion at 36. As the Court explained, if the FISA application "articulates a broader objective than criminal prosecution – such as stopping an ongoing conspiracy – and includes other potential non-prosecutorial responses, the government meets the statutory test." *Id.* at 36. The government should be able to meet that test, even when prosecution is its dominant motive.

As to the second requirement, as a practical matter it becomes an issue only when an FI or FCI investigation reveals a serious crime that is not related to foreign intelligence. That does not often occur, because most serious crimes committed by agents of foreign powers are in fact related to their foreign intelligence activities – e.g., international terrorists tend to commit terrorism-related offenses (including crimes committed to fund or facilitate terrorism), and foreign spies tend to commit espionage-related offenses (including crimes committed to fund or facilitate espionage). When the issue does arise, it may be appropriate for the FISA application to explain why prosecution of that unrelated crime is not the primary purpose of the search or surveillance. But it is important to remember that an agent of a foreign power is not immunized against FISA surveillance merely because he also commits an ordinary crime. Agents and prosecutors should not fear coordinating merely because an ordinary crime has been discovered.

b. The Court of Review's decision further encourages coordination by changing the nature and scope of judicial inquiry into the government's purpose for using FISA. Under prior law, as noted above, the FISC determined the government's purpose by reviewing consultations and coordination between line attorneys and agents, and compared intelligence and law enforcement purposes to find which one was primary. The Court of Review flatly rejected that approach. It held that the Patriot Act "eliminated any justification for the [FISC] to balance the relative weight the government places on criminal prosecution as compared to other counterintelligence responses." Opinion at 36. Thus, the significance of a foreign intelligence purpose is judged on its own terms, and does not vary according to the significance of a law enforcement purpose.

More importantly, the Court of Review also held that the government's purpose is determined by the high-level certification that is a part of every FISA application, not the coordination between line attorneys and agents in the field. Thus, the Court held, the significant purpose test is "not a standard whose application the [FISC] legitimately reviews by seeking to inquire into which Justice Department

Subject: A Summary of the FISA Appeal Decision

officials" – law enforcement or intelligence – "were instigators of an investigation" or a request to use FISA. Opinion at 38. Rather, "the government's purpose * * * is to be judged by the national security official's articulation [in the FISA certification], and not by a [FISC] inquiry into the origins of an investigation nor an examination of the personnel involved." *Id.* at 37-38. The "relevant purpose is that of those senior officials in the Executive Branch who have the responsibility of appraising the government's national security needs," and if the Attorney General "wishes a particular investigation to be run by an officer of any division, that is his prerogative." *Id.* at 38. Where the FISC has doubts, "it can demand further inquiry into the certifying officer's purpose," but an inquisition of line attorneys and agents would be inappropriate because the certification represents the government's purpose regardless of "whatever may be the subjective intent of the investigators or lawyers who initiate an investigation." *Id.* at 38, 36.

In keeping with that analysis, the Court of Review rejected the FISC's new Rule 11. Rule 11 required every FISA application to include "informative descriptions of any ongoing criminal investigations of FISA targets, as well as the substance of any consultations between the FBI and criminal prosecutors at the Department of Justice or a United States Attorney's Office." Descriptions of ongoing criminal investigations are unnecessary because the significant purpose test does not require a comparison between intelligence and law enforcement motives. Descriptions of consultations among agents and prosecutors are unnecessary because the relevant purpose under FISA is determined by the certifying official and the Attorney General.

In sum, the Court of Review's decision allows unprecedented coordination between intelligence and law enforcement officials, and should assist the Department of Justice in using all available resources, intelligence and law enforcement alike, to protect the country against foreign spies and terrorists. If you have any questions about the meaning or application of the Court's decision, or the March 2002 Intelligence Sharing Procedures, please contact the FBI's National Security Law Unit, the Criminal Division, or OIPR.